6. Cardinality

Definitions and Preliminary Examples

Suppose that $\mathscr{S}$ is a non-empty collection of sets. We define a relation $\approx$ on $\mathscr{S}$ by $A \approx B$ if and only if there exists a one-to-one function f from A onto B (sometimes called a **bijection**). That is, A and B are in **one-to-one correspondence**.

1. Show that $\approx$ is an equivalence relation on $\mathscr{S}$.

Two sets that are in one-to-one correspondence are said to have the same **cardinality**. Thus, the equivalence classes under this equivalence relation capture the notion of having the same number of elements.

For $k \in \mathbb{N}$, let $\mathbb{N}_k = \{0, 1, \ldots, k - 1\}$. Technically, a set A is **finite** if $A \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$, in which case k is the cardinality of A, and we write $\#(A) = k$. Think of $\mathbb{N}_k$ as a *reference set* with k elements; any other set with k elements must be equivalent to this one. Appropriately enough, a set is **infinite** if it's not finite. We will study the cardinality of finite sets in the next two sections on Counting Measure and Combinatorial Structures. In this section, we will concentrate primarily on infinite sets.

2. Let S be a set. Recall that $\mathscr{P}(S)$ denotes the power set of S (the set of all subsets of S), and $\{0, 1\}^S$ denotes the set of functions from S into $\{0, 1\}$. Show that $\mathscr{P}(S) \approx \{0, 1\}^S$. The mapping that takes a set A into its indcator function $\mathbf{1}(A)$ is a bijection.

A set that is equivalent to the set of natural numbers $\mathbb{N}$ is said to be **countably infinite**. A set that is either finite or countably infinite is said to be **countable**. Countable sets play a very important role in probability theory, as in many other branches of mathematics. Appropriately enough, a set that is not countable is said to be **uncountable**. We will soon see that there *are* such sets.

3. Show that the set of even natural numbers $E = \{0, 2, 4, \ldots\}$ is countable infinite, and the set of integers $\mathbb{Z}$ is countable infinite.

a. A one-to-one mapping from $\mathbb{N}$ onto E can be constructed by mapping n to $2n$
b. A one-to-one mapping from $\mathbb{N}$ onto $\mathbb{Z}$ can be constructed by mapping the even natural numbers one-to-one onto the natural numbers, and the odd natural numbers one-to-one onto the negative integers.

4. Suppose that A is a set with at least two elements, and let $S = A^{\mathbb{N}}$, the set of all functions from $\mathbb{N}$ into A. Thus, the elements of S are infinite sequences indexed by $\mathbb{N}$ and taking values in A. Show that S is uncountable. The proof is by contradiction, and uses a nice trick known as the **diagonalization** method:

a. Suppose that S is countably infinite (it's clearly not finite), so that the elements of S can be enumerated: $S = \{f_0, f_1, f_2, \ldots\}$
b. Now construct a new function g that differs from every function in the list. Specifically, suppose that a and b are

distinct elements of A. Define $g : \mathbb{N} \to A$ by $g(n) = b$ if $f_n(n) = a$ and $g(n) = a$ if $f_n(n) \neq a$

c. Show that $g \neq f_n$ for each $n \in \mathbb{N}$, which contradicts the fact that S is the set of *all* functions from $\mathbb{N}$ into A.

Subsets of Infinite Sets

Surely a set must be as least as large as any of its subsets, in terms of cardinality. On the other hand, it might also seem that the set of even natural numbers is only half the size of the set of all natural numbers, and that the set of integers is twice the size of the set of natural numbers. However, by a Exercise 3, the three sets have exactly the same size, in terms of cardinality. In this subsection, we will explore some interesting and somewhat paradoxical results that relate to subsets of infinite sets. Along the way, we will see that the countable infinity is the "smallest" of the infinities.

5. Suppose that S is an infinite set. Show that S has a countable infinite subset.

a. Select $a_0 \in S$. It's possible to do this since S is nonempty.
b. Inductively, having chosen $\{a_0, a_1, \ldots, a_{k-1}\} \subseteq S$, select $a_k \in S \setminus \{a_0, a_1, \ldots, a_{k-1}\}$. Again, it's possible to do this since S is not finite.
c. Manifestly, $\{a_0, a_1, a_2, \ldots\}$ is a countably infinite subset of S.

6. Show that a set S is infinite if and only if S is equivalent to a proper subset of S

a. If S is finite, then S is not equivalent to a proper subset by the "pigeonhole principle"
b. If S is infinite, then S has countably infinite subset $\{a_0, a_1, a_2, \ldots\}$ by the previous exercise. Show that S is equivalent to $S \setminus \{a_1, a_3, a_5, \ldots\}$. Construct the bijection as follows:
c. Map $\{a_0, a_1, a_2, \ldots\}$ one-to-one onto $\{a_0, a_2, a_4, \ldots\}$. This can be done in essentially the same way that the natural numbers were mapped one-to-one onto the even natural numbers in Exercise 3.
d. For every other element $x \in S \setminus \{a_0, a_2, a_4, \ldots\}$, map x to x.

When S was infinite in the previous exercise, not only did we map S one-to-one onto a proper subset, we actually threw away a countably infinite subset and still maintained equivalence. Similarly, we can *add* a countably infinite set to an infinite set S without changing the cardinality S.

7. Show that if S is an infinite set and B is a countable set, then $S \approx S \cup B$

a. Consider the most extreme case where B is countably infinite and disjoint from S.
b. S has a countably infinite subset $A = \{a_0, a_1, a_2, \ldots\}$, and $B = \{b_0, b_1, b_2, \ldots\}$. Construct the bijection as follows:
c. Map the even order terms of A one-to-one onto A, and map the odd order terms of A one-to-one onto B.
d. For every element $x \in S \setminus A$, map x to x

In particular, if S is uncountable and B is countable then $S \cup B$ and $S \setminus B$ have the same cardinality as S, and in particular are uncountable.

In terms of the dichotomies *finite-infinite* and *countable-uncountable*, a set is indeed at least as large as a subset. First we need a preliminary result.

8. Show that if S is countably infinite and A is an infinite subset of S, then A is countably infinite.

a. Since S is countably, it can be enumerated: $S = \{x_0, x_1, x_2, \ldots\}$
b. Let n_i be the i^{th} smallest index such that $x_{n_i} \in A$
c. Argue that $A = \left\{x_{n_0}, x_{n_1}, x_{n_2}, \ldots\right\}$ and hence is countably infinite.

9. Suppose that $A \subseteq B$. Prove the following results.

a. If B is finite then A is finite.
b. If A is infinite then B is infinite.
c. If B is countable then A is countable.
d. If A is uncountable then B is uncountable.

Hint: Note that (b) is the contrapositive of (a), and (d) is the contrapositive of (c).

Comparisons by one-to-one and onto functions

We will look deeper at the general question of when one set is "at least as big" than another, in the sense of cardinality. Not surprisingly, this will eventually lead to a partial order on the cardinality equivalence classes

First note that if there exists a function that maps a set A one-to-one into a set B, then, in a sense, there is a copy of A contained in B. Hence B should be at least as large as A.

10. Suppose that $f : A \to B$ is one-to-one. Show that

a. If B is finite then A is finite.
b. If A is infinite then B is infinite.
c. If B is countable then A is countable.
d. If A is uncountable then B is uncountable.

Hint: Note that f maps A one-to-one onto $f(A)$, and $f(A) \subseteq B$. Now use the Exercise 9.

On the other hand, if there exists a function that maps a set A onto a set B, then, in a sense, there is a copy of B contained in A. Hence A should be at least as large as B.

11. Suppose that $f : A \to B$ is onto. Show that

a. If A is finite then B is finite.
b. If B is infinite then A is infinite.
c. If A is countable then B is countable.
d. If B is uncountable then A is uncountable.

Hint: For each $y \in B$, select a specific $x \in A$ with $f(x) = y$ (if you are persnickety, you may need to invoke the axiom of choice). Let C be the set of chosen points. Argue that f maps C one-to-one onto B, and $C \subseteq A$. Now use the Exercise 10.

The previous exercise also could be proved from the one before, since if there exists a function f mapping A onto B, then there exists a function g mapping B one-to-one into A. This duality is proven in the discussion of the axiom of choice. A simple and useful corollary of the previous two theorems is that if B is a given countably infinite set, then a set A is countable if and only if there exists a one-to-one function f from A into B, if and only if there exists a function g from B onto A.

12. Show that if A_i is a countable set for each i in a countable index set I, then $\bigcup_{i \in I} A_i$ is countable.

a. Consider the most extreme case in which the index set I is countably infinite.
b. There exists a function f_i that maps $\mathbb{N}$ onto A_i for each $i \in \mathbb{N}$.
c. Let $M = \left\{2^i\, 3^j : (i \in \mathbb{N}) \text{ and } (j \in \mathbb{N})\right\}$. Note that M is countably infinite.
d. Define $f : M \to \bigcup_{i \in I} A_i$ by $f\left(2^i\, 3^j\right) = f_i(j)$. Show that f is well-defined and is onto.

13. Show that if A and B are countable then $A \times B$ is countable.

a. There exists a function f that maps $\mathbb{N}$ onto A, and there exists a function g that maps $\mathbb{N}$ onto B.
b. Again, let $M = \left\{2^i\, 3^j : (i \in \mathbb{N}) \text{ and } (j \in \mathbb{N})\right\}$. Note that M is countably infinite.
c. Define $h : M \to A \times B$ by $h\left(2^i\, 3^j\right) = (f(i), g(j))$. Show that h is well-defined and is onto.

The last result could also be proven from the one before, by noting that

$$A \times B = \bigcup_{a \in A} \{a\} \times B$$

Both proofs work because the set M is essentially a copy of $\mathbb{N} \times \mathbb{N}$, embedded inside of $\mathbb{N}$. The last theorem generalizes to the statement that a finite product of countable sets is still countable. But, from Exercise 4, a product of *infinitely* many sets (with at least 2 elements each) will be uncountable.

14. Show that the set of rational numbers $\mathbb{Q}$ is countably infinite.

a. The sets $\mathbb{Z}$ and $\mathbb{N}_+$ are countably infinite.
b. The set $\mathbb{Z} \times \mathbb{N}_+$ is countably infinite.
c. The function $f : \mathbb{Z} \times \mathbb{N}_+ \to \mathbb{Q}$ given by $f(m, n) = \frac{m}{n}$ is onto.

A real number is **algebraic** if it is the root of a polynomial function (of degree 1 or more) with integer coefficients. Rational numbers are algebraic, as are rational roots of rational numbers (when defined). Moreover, the algebraic numbers are closed under addition, multiplication, and division. A real number is **transcendental** if it's not algebraic. The numbers e and π are transcendental, but we don't know very many other transcendental numbers by name. However, as we will see, most (in the sense of cardinality) real numbers are transcendental.

15. Show that the set of algebraic numbers $\mathbb{A}$ is countably infinite.

a. Let $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$ and let $\mathbb{Z}_n = \mathbb{Z}^{n-1} \times \mathbb{Z}_0$ for $n \in \mathbb{N}_+$. The set $\mathbb{Z}_n$ is countably infinite for each n.
b. Let $C = \bigcup_{n=1}^\infty \mathbb{Z}_n$. Think of C as the set of coefficients; C is countably infinite.
c. Let P denote the set of polynomials of degree 1 or more, with integer coefficients. The function $(a_0, a_1, \ldots, a_n) \mapsto a_0 + a_1 x + \cdots + a_n x^n$ maps C onto P.
d. A polynomial of degree n in P has at most n roots, by the fundamental theorem of algebra.

Now let's look at some uncountable sets.

16. Show that the interval $[0, 10)$ is uncountable.

a. Let S denote the set of all functions from $\mathbb{N}$ into $\{0, 1, 2, \ldots, 9\}$, thought of as infinite sequences. The set S is uncountable.
b. Let N denote the set of all sequences in S that eventually end in all 9's. The set N is countably infinite.
c. The set $D = S \setminus N$ has the same cardinality as S, and in particular is uncountable.
d. The mapping f that takes a sequence in D and returns the corresponding decimal expansion $f(\boldsymbol{x}) = x_0.x_1 x_2 x_3 \ldots$ is a bijection from D onto $[0, 10)$.

17. Show that the following sets have the same cardinality, and in particular all are uncountable:

a. $\mathbb{R}$, the set of real numbers.
b. Any interval I of $\mathbb{R}$, as long as the interval is not empty or a single point.
c. $\mathbb{R} \setminus \mathbb{Q}$, the set of irrational numbers.
d. $\mathbb{R} \setminus \mathbb{A}$, the set of transcendental numbers.
e. $\mathscr{P}(\mathbb{N})$, the power set of $\mathbb{N}$.

Hints: You can find a linear function that maps an interval one-to-one onto another interval, as long as the two intervals are of the same type--that is, both bounded or unbounded, and both with the same type of closure. A closed (or half-closed) interval differs from its open counterpart by two (or one) points. The natural log function maps the interval $(0, \infty)$ one-to-one onto $\mathbb{R}$. The tangent function maps the interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ one-to-one onto $\mathbb{R}$. The irrational numbers can be obtained from the real numbers by removing the rational numbers (a countably infinite set), and similarly, the transcendental numbers can be obtained from the real numbers by removing the algebraic numbers (again a countably infinite set).

The Cardinality Partial Order

Suppose that $\mathcal{S}$ is a nonempty collection of sets. We define the relation $\preceq$ on $\mathcal{S}$ by $A \preceq B$ if and only if there exists a one-to-one function f from A into B, if and only if there exists a function g from B onto A. In light of the previous subsection, $A \preceq B$ should capture the notion that B is at least as big as A, in the sense of cardinality.

18. Show that $\preceq$ is reflexive and transitive.

Thus, we can use the construction in the section on on Equivalence Relations to first define an equivalence relation on $\mathcal{S}$, and then extend $\preceq$ to a true partial order on the collection of equivalence classes. The only question that remains is whether the equivalence relation we obtain in this way is the same as the one that we have been using in our study of cardinality. Rephrased, the question is this: *If there exists a one-to-one function from A into B and a one-to-one function from B into A, does there necessarily exist a one-to-one function from A* ***onto*** *B?* Fortunately, the answer is yes; the result is known as the **Schröder-Bernstein Theorem**, named for Ernst Schröder and Sergi Bernstein.

19. Show that if $A \preceq B$ and $B \preceq A$ then $A \approx B$.

a. Set inclusion $\subseteq$ is a partial order on $\mathcal{P}(A)$ (the power set of A) with the property that every subcollection of $\mathcal{P}(A)$ has a supremum (namely the union of the subcollection).
b. Suppose that f maps A one-to-one into B and g maps B one-to-one into A. Define the function $h : \mathcal{P}(A) \to \mathcal{P}(A)$ by $h(U) = A \setminus g(B \setminus f(U))$ for $U \subseteq A$.
c. Show that h is increasing: if $U \subseteq V$ then $h(U) \subseteq h(V)$
d. Use the fixed point theorem for partially ordered sets to conclude that there exists $U \subseteq A$. such that $h(U) = U$.
e. Conclude that $g(B \setminus f(U)) = A \setminus U$.
f. Now define $F : A \to B$ by $F(x) = f(x)$ if $x \in U$ and $F(x) = g^{-1}(x)$ if $x \in A \setminus U$. Show that F is one-to-one and onto.

We will write $A \prec B$ if $A \preceq B$, but A and B are not equivalent. That is, there exists a one-to-one function from A into B, but there does not exist a function from A onto B. Note that $\prec$ would have its usual meaning if applied to the equivalence classes. That is, $[A] \prec [B]$ if and only if $[A] \preceq [B]$ but $[A] \neq [B]$. Intuitively, of course, $A \prec B$ means that B is strictly larger than A, in the sense of cardinality.

20. Show that $A \prec B$ in each of the following cases:

a. A and B are finite and $\#(A) < \#(B)$
b. A is finite and B is countably infinite.
c. A is countably infinte and B is uncountable.

We close our discussion with the observation that for any set, there is always a larger set.

21. Let S be a set. Show that $S \prec \mathcal{P}(S)$.

a. First, it's trivial to map S one-to-one *into* $\mathcal{P}(S)$; just map x to $\{x\}$.
b. Suppose that f maps S onto $\mathcal{P}(S)$ and let $R = \{x \in S : x \notin f(x)\}$. Since f is onto, there exists $t \in S$ with $f(t) = R$.
c. Show that $t \in f(t)$ if and only if $t \notin f(t)$.

The proof that a set cannot be mapped onto its power set is similar to the **Russell paradox**, named for Bertrand Russell.

The **continuum hypothesis** is the statement that there is no set of real numbers whose cardinality is between between that of $\mathbb{N}$ and $\mathbb{R}$. The continuum hypothesis actually started out as the continuum *conjecture*, until it was shown to be consistent with the usual axioms of the real number system (by Kurt Gödel in 1940), and independet of those axioms (by Paul Cohen in 1963).
